MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MIT 2.111/8.411/6.898/18.435
Quantum Information Science I

October 21, 2010

Problem Set #6
(due in class, 28-Oct-10)

1. **Building controlled-U from U.**

   Suppose you are given a box which performs a unitary gate U on a one-qubit input state. In addition, you are given $|u\rangle$, and eigenstate of U with eigenvalue one.

   (a) Provide a quantum circuit using quantum Fredkin (ie controlled-swap) gates, which peforms a controlled-U gate, using this box, and $|u\rangle$.

   (b) Can you use the same approach if $|u\rangle$ has some known eigenvalue $e^{i\phi}$?

   (c) What if ϕ is unknown?

2. **The Gottesman-Knill Theorem**. An important result in quantum computation is that H, CNOT, and the Pauli gates are not universal for quantum computation, and in fact any quantum circuit composed from those gates (together with standard input states and measurements in the computational basis) can be simulated efficiently by a classical computer! This result is known as the *Gottesman-Knill* theorem, and in this problem we prove the essential result behind the theorem.

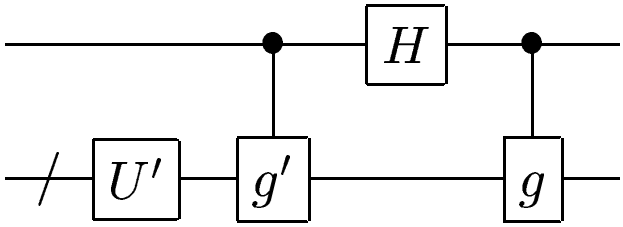
   Let G_n denote the Pauli group on n qubits, that is, matrix multiplication acting on the set of n-fold tensor products of Pauli matrices (including multiplicative factors $\pm 1, \pm i$). By definition, we say the set of U such that $UG_nU^\dagger = G_n$ is the *normalizer* of G_n, and denote it by $N(G_n)$. The following theorem about the normalizer of the Pauli group holds:

   > Suppose U is any unitary operator on n qubits with the property that if $g \in G_n$ then $UgU^\dagger \in G_n$. Then up to a global phase U may be composed from $O(n^2)$ Hadamard, phase and controlled-NOT gates.

   We can construct an inductive proof of this theorem as follows:

   (a) Prove that the Hadamard and phase gates (H and S) can be used to perform any normalizer operation on a single qubit.

   (b) Suppose U is an $n+1$ qubit gate in $N(G_{n+1})$ such that $UZ_1U^\dagger = X_1 \otimes g$ and $UX_1U^\dagger = Z_1 \otimes g'$ for some $g, g' \in G_n$. Define U' on n qubits by $U'|\psi\rangle \equiv \sqrt{2}\langle 0|U(|0\rangle \otimes |\psi\rangle)$. Use the inductive hypothesis to show that this construction for U:

   may be implemented using $O(n^2)$ Hadamard, phase and controlled-NOT gates.

   (c) Show that any gate $U \in N(G_{n+1})$ may be implemented using $O(n^2)$ Hadamard, phase and controlled-NOT gates.